Como manter seus boletos seguros

Com a presença e sofisticação crescentes de ameaças online, como vírus, ransomware e golpes de phishing, é importante ter ações preventivas e mitigar os problemas relacionados a fraudes de boletos.

1. Evitar vírus e golpes de phishing

35%

Malwares e vírus atacam seu computador ao visitar sites mal-intencionados ou baixar arquivos infectados. 35% de todos os computadores globais são infectados por malware.

23%

Os hackers usam scams de phishing para tentar roubar sua identidade ou o seu dinheiro enviando e-mails de aparência oficial para obter informações pessoais confidenciais. 23% das pessoas abrem e-mails de phishing*.

Fonte: Microsoft.

* Phishing: termo em inglês que significa “pescar”. Consiste em espalhar várias mensagens em massa para uma grande lista de contatos, esperando que alguém “morda a isca, visando obter dados pessoais.

2. Como são feitos os golpes

1. O golpe mais comum é você receber um e-mail com um boleto anexo, de alguma empresa como operadoras de telefonia, cartão de crédito, registro de domínios, planos de saúde, multas de trânsito, que em geral estes são mais fáceis de serem percebidos. Fique atento ao remetente, a data de vencimento, valores, erros de ortografia, logos entre outros aspectos. Normalmente as notificações relacionadas a multas, processos judiciais são feitos via correios nunca por e-mail.

2. Outra forma comum de golpe é através de vírus (malwares), instalado no computador do usuário que altera as configurações do arquivo quando aberto.

3. Contudo, estes golpes evoluíram ficaram mais sofisticados. O foco maior são empresas, onde os cibercrimonosos interceptam a conta de e-mail do destinatário. Esta interceptação permite o acesso ao e-mail, os golpistas alteram a mensagem e os arquivos PDF´s, mudando códigos de barras e até mesmo o QRCODE de PIX. Os cibercriminosos utilizam-se de falhas nos provedores de e-mail, vazamento de contas, senhas fracas e criam um banco de dados de contas de e-mail que são monitoradas.

Obtenção de acesso ao e-mail: Os golpistas obtêm acesso não autorizado à conta de e-mail da vítima. Isso pode ser feito por meio de técnicas de phishing, malware ou engenharia social, onde os golpistas enganam a vítima para que revele suas credenciais de login.

Monitoramento das comunicações: Após obter acesso ao e-mail da vítima, os golpistas monitoram as comunicações em busca de informações sobre transações financeiras, como pagamento de contas ou faturas. O título do assunto ajuda localizar as mensagens com boletos e de interesse dos golpistas.

Identificação de boletos: Os golpistas identificam boletos de pagamento que foram enviados para a vítima por e-mail. Isso pode incluir boletos de serviços, compras online ou faturas de empresas.

Manipulação dos boletos: Os golpistas interceptam os e-mails contendo os boletos de pagamento e os modificam. Eles alteram os detalhes de pagamento, como o valor do boleto, o beneficiário ou o número da conta bancária, redirecionando assim o pagamento para uma conta controlada pelos golpistas.

Reenvio do boleto fraudado: Após a manipulação do boleto, os golpistas reenviam o e-mail para a vítima, muitas vezes utilizando técnicas de spoofing para fazer com que o e-mail pareça legítimo.

Pagamento fraudulento: A vítima, ao receber o boleto fraudado, realiza o pagamento conforme as instruções fornecidas no boleto modificado, transferindo assim o valor para a conta dos golpistas.

As contas corporativas são mais valiosas que as contas de usuários domésticos, pois o consumo e tarifa são maiores.

2. Quais ferramentas são usadas por cibercriminosos?

Phishing é um crime cibernético que visa roubar informações confidenciais. Os hackers se disfarçam (spoofing) de grandes corporações ou de entidades confiáveis para induzir você a fornecer voluntariamente informações como credenciais de login e senha de e-mail, números de cartões de crédito.

Estas ferramentas utilizadas para golpes são os vírus (malwares), este normalmente são instalados no computador do usuário, quando este abre algum arquivo infectado. O mais comum são arquivos e links que vêm por meio de e-mails, o usuário clica no link ou abre um anexo e pronto, vírus instalado.

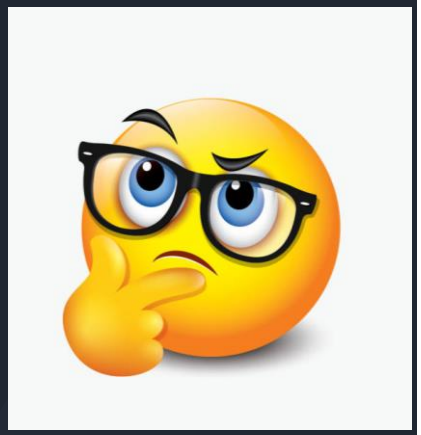
Você já ouviu falar do **Reboleto**? Este é um software usado pelos cibercriminosos para capturar, interceptar contas de e-mails.

Este software é comercializado na internet em fóruns clandestinos, grupos de Telegram e WhatsApp. Após a captura do e-mail, o cibercriminoso poderá realizar a abertura do e-mail com o intuito de alterar o corpo do e-mail e anexos, como o documento PDF anexado.

Depois de acessar o e-mail é feita a edição do documento PDF. Usando um editor, como o Foxit PDF Editor, o documento é alterado trocando o código de barras e QRCODE PIX. Após salvar o arquivo, este será anexado automaticamente ao e-mail interceptado e, em sequência é feito o envio ao destinatário correto.

Também é possível verificar que na caixa de mensagem do destinatário o e-mail chega normalmente porém, com outra data e hora e com o conteúdo do PDF totalmente alterado pelo criminoso. Este processo de alteração é todo manual.

"O único momento de evitar o golpe é na hora de pagar a conta, pois é possível perceber a alteração no nome do destinatário, seja após a leitura do código de barra ou via o QR-Code do Pix". Fonte Kaspersky.



-----Mensagem original-----
De: xxxxx [mailto:contato4@si-cobra.com] Enviada em: quinta-feira, 05 de novembro de 2023 01:11
Para: SERVICOS JOAO LTDA
Assunto: IMPORTANTE - Corre o de T tulo: 001, Valor:R$ 3446,50, Venc.: 05/11/2023

Prezado(a),

Informamos a SERVICOS JOAO LTDA, que devido a problemas operacionais em nosso sistema de emissão de Notas Fiscais, foi constatado um erro na base de cálculo da alíquota de ICMS/Pis sendo que foi cobrado a mais o valor de R$ 364,26, referente à Nota fiscal de Nº 11224, Chave NFe 32221020000001000002005001000000000000002009091.
Como forma de neutralizar o erro de nosso sistema, estaremos bonificando com um crédito de R$ 526,00 no título 001 com data de vencimento para 24/11/2023.
Pedimos que desconsidere o boleto anterior (NÃO PAGUE) de R$ 3446,50 em DDA e utilize o NOVO BOLETO EM ANEXO com o valor retificado de R$ 2,920,50
Solicitamos por gentileza que confirme o recebimento deste email.

OBS.: Crédito/Bonificação referente a divergência na cobrança da alíquota de Cofins/PIS/IPI cobrado a mais.
Encontra-se em anexo a Baixa do Título Anterior e o Novo Boleto Atualizado com a devida dedução.

Att,

Mariana Santos
Dpto. Financeiro

3. Exemplo de fraude

No exemplo acima, o e-mail foi interceptado. O corpo do e-mail foi alterado, informando que houve um erro de cálculo de imposto e, por isso, foi concedido um desconto. O boleto em anexo, também foi alterado e enviado com o novo valor.

Isto demonstra bem a criatividade dos golpistas, pois apelam para gatilhos mentais como ganho financeiro e confiança, quando reportam o erro no cálculo do imposto e reduzem o valor.

4. Como prevenir e diminuir a possibilidade de fraudes

Mantenha sempre softwares originais na empresa.

Backup regular: Faça backup regularmente dos seus e-mails e mantenha cópias de segurança armazenadas em locais seguros. Isso pode ajudar a recuperar suas informações em caso de comprometimento.

Se receber um boleto suspeito, entre em contato diretamente com a empresa ou instituição financeira que supostamente emitiu o boleto para verificar sua autenticidade.

Cuidado com o texto do assunto evite mencionar boleto, pagamento, nota fiscal e termos relacionados.

Utilize provedores de e-mails confiáveis e com políticas de segurança atualizada. Exija a comprovação de que os métodos de segurança são aplicados.

Use senhas fortes: Mantenha suas contas de e-mail protegidas com senhas difíceis e únicas, misturando letras maiúsculas e caracteres especiais. Evite usar senhas fáceis de adivinhar e altere-as regularmente.

A melhor prevenção é educar-se.

4.1 Como prevenir e diminuir a possibilidade de fraudes

Treinamento de conscientização em segurança: Eduque-se e eduque sua equipe sobre as práticas recomendadas de segurança cibernética, para reconhecer e evitar ameaças comuns, como phishing e engenharia social.

Informe regularmente seus clientes, parceiros e fornecedores sobre sua conta de e-mail, banco para pagamento, razão social e CNPJ para que fiquem atentos

Verifique sempre a autenticidade de boletos recebidos, especialmente se parecerem suspeitos. Confira os detalhes, como o nome do beneficiário, o valor e o código de barras.

Evite abrir links ou baixar arquivos de e-mails ou mensagens de texto não solicitados. Eles podem conter malware projetado para comprometer sua segurança.

Mantenha seu software antivírus e antimalware atualizado em todos os dispositivos.

Ao adotar essas estratégias de segurança, você pode reduzir significativamente o risco de ter sua conta de e-mail interceptada e comprometida por indivíduos mal-intencionados.

Vigilância constante e educação são as melhores defesas contra fraudes por e-mail.

5. Métodos de segurança para envio de e-mail

Recentemente Google e Yahoo adotaram novas práticas para receberem e-mails de outros provedores. São medidas de segurança adotadas para evitar problemas de SPAM e disseminação de vírus e fraudes. Isto está obrigando com que muitos provedores se adaptem as novas regras.

- **Quais são estas regras:**

São protocolos/métodos/políticas de segurança que visam inibir ações como: interceptação do e-mail por cibercriminosos, alterações de conteúdo, alterações de remetentes, spam entre outros tipos de fraudes, ataques e armadilhas por e-mail, estes métodos são: SPF, DKIM e DMARC.

- **O que acontece se meu provedor não dispõe de tais recursos?**

Seus e-mails ***deixam*** de ser entregues para os provedores que utilizam estas políticas ou seus e-mails serão encaminhados para caixa de spam automaticamente.

- **Em resumo:**

❑ SPF: Verifica a origem do e-mail.

❑ DKIM: Verifica a autenticidade do remetente.

❑ DMARC: Define o que fazer com e-mails que falham na autenticação.

Para saber mais clique:

O que é um registro de DNS DKIM? | Cloudflare

Antispam.br ::

➔ Aproveite e baixe nosso material abordando estes métodos exigidos pelo Google e Yahoo. Inclusive tem um link para uma ferramenta para você testar a segurança de seu e-mail.

Repasse para sua equipe, clientes, fornecedores e parceiros. Clique no link a seguir para baixar.

seguranca_e-mail.pdf (softilux.com.br)

6. O que diz a legislação

Destaca-se que as instituições financeiras têm o dever de implementar medidas de segurança para proteger os clientes, enquanto as empresas emissoras de boletos devem assegurar a integridade de seus sistemas, processos e segurança da informação para evitar fraudes. Os consumidores também têm responsabilidades, como verificar a autenticidade dos boletos e proteger suas informações pessoais durante transações online.

Porém, o Marco Civil da Internet não especifica diretamente a responsabilidade sobre fraudes digitais de boletos, sendo regulado por outras legislações, como o Código de Defesa do Consumidor e o Código Civil Brasileiro.

A discussão sobre a responsabilidade das instituições bancárias levou ao estabelecimento de jurisprudência pelo STJ, por meio da Súmula 479. Esta súmula estabelece a responsabilidade objetiva dos bancos por danos causados por fraude ou incidentes internos durante operações bancárias. A imposição desse ônus decorre do controle que os bancos têm sobre as operações online e da obrigação de observar a qualidade e segurança de seus serviços, conforme estabelecido no Código de Defesa do Consumidor.

Conheça seus direitos, busque apoio especializado se necessário.

7. Conclusão

Em um mundo digital cada vez mais interconectado, a segurança de nossas comunicações por e-mail é de suma importância. Ao longo deste eBook, exploramos as diversas maneiras pelas quais indivíduos e organizações podem ser alvos de ataques cibernéticos, desde phishing até malware e engenharia social.

No entanto, ao entender os riscos e adotar práticas recomendadas de segurança, podemos reduzir significativamente a probabilidade de se tornar vítima de fraudes e ataques de e-mail. Desde o uso de criptografia e autenticação de dois fatores até a educação contínua sobre phishing e a importância de senhas fortes. Cada passo que damos em direção à segurança fortalece nossas defesas contra ameaças cibernéticas.

Lembre-se, a segurança de e-mail é uma responsabilidade compartilhada. Ao adotarmos medidas preventivas em nossas próprias práticas de comunicação e incentivarmos outros a fazerem o mesmo, podemos criar um ambiente mais seguro e protegido para todos. Esteja sempre alerta, proteja suas informações pessoais e empresariais e lembre-se de que a segurança cibernética é um esforço contínuo. Juntos, podemos construir um futuro digital mais seguro e confiável.

Obrigado

Queremos agradecer o seu interesse e esperamos de alguma forma ter contribuído para ajudar você e a sua empresa.

Não deixe de entrar em contato em caso de dúvida e nos acompanhe no instagram.

Até o próximo e-book

Softilux sistemas

https://softilux.com.br/

48) 99983-1345

comercial@softilux.com.br

Para acessar nosso Instagram clique aqui